

US-PAT-NO: 5850446

DOCUMENT-IDENTIFIER: US 5850446 A

TITLE: System, method and article of
manufacture for virtual point of sale processing utilizing an
extensible, flexible architecture

----- KWIC -----

Detailed Description Text - DETX (33):

Frameworks also represent a change in the way
programmers think about the
interaction between the code they write and code written by
others. In the
early days of procedural programming, the programmer called
libraries provided
by the operating system to perform certain tasks, but
basically the program
executed down the page from start to finish, and the
programmer was solely
responsible for the flow of control. This was appropriate
for printing out
paychecks, calculating a mathematical table, or solving
other problems with a
program that executed in just one way.

Detailed Description Text - DETX (92):

In function block 620, payment gateway computer system
140 verifies merchant
computer system's 130 encryption public key certificate 515
and merchant
computer system's 130 signature public key certificate 520.
Payment gateway
computer system 140 performs this verification by making a
call to the
certification authorities associated with each certificate.
If verification of
either certificate fails, payment gateway computer system
140 rejects the

authorization request.

Detailed Description Text - DETX (93):

In function block 625, payment gateway computer system 140 validates merchant digital signature 525. Payment gateway computer system 140 performs this validation by calculating a message digest over the contents of the combined basic authorization request 510, the encryption public key certificate 515 and the signature public key certificate 520. Payment gateway computer system 140 then decrypts digital signature 525 to obtain a copy of the equivalent message digest calculated by merchant computer system 130 in function block 420. If the two message digests are equal, the digital signature 525 is validated. If validation fails, payment gateway computer system 140 rejects the authorization request.

Detailed Description Text - DETX (121):

FIG. 12 depicts the detailed steps of processing a payment capture request and generating and transmitting a payment capture request response. Function blocks 1210 through 1245 depict the steps of processing a payment capture request, while function blocks 1250 through 1285 depict the steps of generating and transmitting a payment capture request response. In function block 1210, payment gateway computer system 140 applies its private key to encrypted random key 1160 contained within received merchant capture request 915, thereby decrypting it and obtaining a cleartext version of random key RK-3 1140. In function block 1215, payment gateway computer system 140 applies random key RK-3 1140 to encrypted combined block 1150, thereby decrypting it and obtaining a cleartext version of combined block 1130. Combined block

1130 comprises
basic capture request 1110, a copy of merchant computer
system's 130 encryption
public key certificate 1115 and a copy of merchant computer
system's 130
signature public key certificate 1120, as well as merchant
digital signature
1125. In function block 1220, payment gateway computer
system 140 verifies
merchant computer system's 130 encryption public key
certificate 1115 and
merchant computer system's 130 signature public key
certificate 1120. Payment
gateway computer system 140 performs this verification by
making a call to the
certification authorities associated with each certificate.
If verification of
either certificate fails, payment gateway computer system
140 rejects the
capture request.

Detailed Description Text - DETX (122):

In function block 1225, payment gateway computer system
140 validates
merchant digital signature 1125. Payment gateway computer
system 140 performs
this validation by calculating a message digest over the
contents of the
combined basic capture request 1110, the encryption public
key certificate 1115
and the signature public key certificate 1120. Payment
gateway computer system
140 then decrypts digital signature 1125 to obtain a copy
of the equivalent
message digest calculated by merchant computer system 130
in function block
1020. If the two message digests are equal, the digital
signature 1125 is
validated. If validation fails, payment gateway computer
system 140 rejects
the capture request. In function block 12 30, payment
gateway computer system
140 applies its private key to encrypted random key RK-2
790 contained within
received merchant capture request 915, thereby decrypting
it and obtaining a

cleartext version of random key RK-2 775. In function block 1235, payment gateway computer system 140 applies random key RK-2 775 to encrypted capture token 780, thereby decrypting it and obtaining a cleartext version of capture token 770.

Detailed Description Text - DETX (334):

This transaction is done at the end of the day to confirm to the host to start the settlement process for the transactions captured by the host for that particular vPOS batch.

Detailed Description Text - DETX (382):

Administrative transaction used to sign-on the vPOS with the host at the start of the day, and also to download encryption keys for debit transactions.

Detailed Description Text - DETX (456):

The reconciliation or close transaction is processed at the end of the day to start the settlement process for the transactions captured by the host for that particular vPOS.

Detailed Description Text - DETX (457):

The host log-on transaction is an administrative transaction which is used to synchronize the vPOS with the host at the start of the day and also initiate a fresh batch at the vPOS terminal.

Detailed Description Text - DETX (461):

The vPOS unlock or start transaction is a local function used to start the vPOS at the start of the day. The vPOS lock or stop function is used to Lock or stop the vPOS from accepting any transactions. The vPOS configuration setup

function is used to setup the vPOS configuration data. The vPOS configuration data is divided into different tables, for example, the Card/Issuer Definition Table (CDT), the Host/Acquirer Definition Table (HDT), the Communications Parameters Table (CPT) and the Terminal Configuration Table (TCT). The following sections explain each of these configuration tables in detail.

Detailed Description Text - DETX (1178):

The Internet is a viable infrastructure for electronic commerce. Ubiquitous browser software for the World Wide Web provides around-the-clock access to a large base of information content provided by Web servers. Utilizing a preferred embodiment, consumers using browsers can shop at virtual stores and malls presented as Web pages managed by the merchants' servers. Consumers can make purchases and pay for them using credit cards or other digital payment instruments in a secure manner. For such Internet-based payments to be authorized, a "gateway" is necessary at the back end to channel transactions to legacy processors and interchange networks.

Detailed Description Text - DETX (1427):

If the request type is either for authorization only or for a sale, execution proceeds with Step 5640. In step 5640, the Gateway initializes a container object to represent the request. In Step 5650, the Gateway extracts the [transaction identifier?] (XID) for the transaction. In Step 5652, the Gateway extracts the merchant identifier (MID) for the transaction. In Step 5654, the Gateway extracts the [what is the RRPID?] (RRPID) and the terminal identifier (TID) for the request. In Step 5656, the Gateway extracts the retry

count associated with the current request. In Step 5660, a message data area is initialized with the extracted contents. The message area can then be used for further processing by the called routine. In Step 5690, the GetSetKeyFields routine returns control to the caller.